

# EXHIBIT 1

Please note that the investigation in this matter is ongoing and this notice may be supplemented with any new significant facts learned subsequent to its submission.

### **Nature of the Data Event**

On January 29, 2019, Covenant Care learned of suspicious activity related to an employee email account. An investigation was immediately commenced to determine the nature and scope of the incident. Covenant Care also immediately took steps to secure the account. Working with third-party forensic investigators, Covenant Care determined that an unauthorized actor(s) gained access to the employee's email account between January 22, 2019 and January 29, 2019. Our investigation determine that the unauthorized actor was able to login to the email account leveraging compromised user credentials. Covenant Care then began a diligent review and analysis of the email account to determine what records were present in the account at the time of unauthorized access, to whom those records relate, and what information the records contained. Through this review, on February 13, 2019, Covenant Care determined that certain patient records were present in the account at the time of the unauthorized access. While the forensic investigation into this incident is ongoing and, to date, Covenant Care is unaware of any actual or attempted misuse of information potentially affected by this incident, it is notifying known, potentially affected individuals out of an abundance of caution.

While the information present at the time of the unauthorized access varies by individual, the information present in the account may include:

- Full name;
- Social Security number or health insurance claim number;
- Date of birth and/or date of death;
- Provider(s) name and treatment location(s);
- Medical record number;
- Diagnoses or diagnosis-related groups (DRGs);
- Dollar amounts billed to Medicare;
- Medicare covered days;
- Admission, re-admission, dates of service, and/or discharge dates; and/or
- Information related to ancillary services, such as home health, hospice, outpatient services, or durable medical equipment.

### **Notice to California Residents**

On March 6, 2019, Covenant Care began providing notice of this incident in writing to seven thousand five hundred eighty-five (7,585) potentially affected California residents and/or their responsible their parties using contact information on record with Covenant Care. Such notice is being provided in substantially the same form as the letter attached here as *Exhibit A*. Covenant Care will also be taking steps to provide notice of this incident to prominent media outlets in California and will be posting notice of this incident on its website in the coming days.

### **Other Steps Taken**

Information privacy and security are of the highest priority for Covenant Care. Upon learning of this incident, steps were quickly taken to secure the affected email account and a thorough investigation was initiated, which is ongoing at this time. The response to this incident includes working with forensic investigators and other third-party vendors to assist with the investigation, mitigation, and remediation activities. Additionally, while strict security safeguards exist to protect patient information, additional technical safeguards are being identified and implemented to enhance security. Further, Covenant Care's

technical, administrative, and physical safeguards are being reviewed to identify and implement any potential enhancements to its security measures. Further, additional employee training is being conducted regarding email safety awareness, and the policies and procedure on employee training on security generally is being reviewed for potential enhancements.

Affected individuals are being offered complimentary access to 12 months of free credit monitoring and identity restoration services. Additionally, potentially affected individuals are being provided with information on how to protect against identity theft and fraud, including information on how to contact the Federal Trade Commission and law enforcement to report any attempted or actual identity theft and fraud. Further, notice of this incident is being provided to the United States Department of Health and Human Services (“HHS”), as well as federal law enforcement and other state regulators as required by law.

By providing this notice, Covenant Care California, LLC does not waive any rights or defenses regarding the applicability of California law, the applicability of the California data incident notification statute, or personal jurisdiction.

# EXHIBIT A

<<ClientDef1(Nursing Facility Name) |>>

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<Zip>>

RE: Notice of Data Privacy Incident

Dear <<FirstName>> <<LastName>>,

<<ClientDef1(Nursing Facility Name)>> is writing to notify you of an incident that may affect the privacy of some of your information. While, to date, we have no evidence that information potentially affected by this incident has been misused, we take this incident very seriously and are providing you with details of the incident and the resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

**What Happened?** Covenant Care California, LLC (“Covenant”) is an affiliated company that provides support services, including administrative and resources assistance, for <<ClientDef1(Nursing Facility Name)>>. On January 29, 2019, Covenant learned of suspicious activity related to an employee email account. We immediately commenced an investigation to determine the nature and scope of the incident. Working with third-party forensic investigators, we determined that an unauthorized actor(s) gained access to the employee’s email account between January 22, 2019 and January 29, 2019. We then undertook a diligent review and analysis of the email account to determine what records were present in the account at the time of unauthorized access, to whom those records relate, and what information the records contained. Through this review, on February 13, 2019, we determined that certain patient records were present in the account at the time of the unauthorized access. Based on our investigation, we determined your information was present in the account. While, to date, we are unaware of any actual or attempted misuse of information potentially affected by this incident, we are providing you this notification out of an abundance of caution.

**What Information Was Affected?** While the information present at the time of the unauthorized access varies by individual, the information present in the account may include your:

- Full name;
- Social Security number or health insurance claim number;
- Date of birth and/or date of death;
- Provider(s) name and treatment location(s);
- Medical record number;
- Diagnoses or diagnosis-related groups (DRGs);
- Dollar amounts billed to Medicare;
- Medicare covered days;
- Admission, re-admission, dates of service, and/or discharge dates; and/or
- Information related to ancillary services, such as home health, hospice, outpatient services, or durable medical equipment.

**What Are We Doing?** Information privacy and security are among our highest priorities. Upon learning of this incident, we quickly took steps to secure the affected email account and initiated a thorough investigation. Our investigation is ongoing and we are working with forensic investigators and other third-party vendors to assist with the investigation, mitigation, and remediation activities. We are also reporting this incident to law enforcement and appropriate state and federal regulators.

<<ClientDef1(Nursing Facility Name)>> has strict security measures in place to protect information in our possession, we are currently reviewing our security policies in response to this incident. We are also planning to perform an overall review of our technical, administrative, and physical safeguards to identify and implement any potential enhancements to our security measures. Further, we are conducting additional employee training on email safety awareness. We are also reviewing our training policies and procedures on security safeguards.

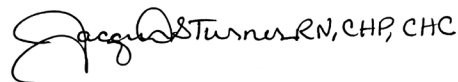
We are providing you with notice of this incident and with information and resources you may use to better protect against potential misuse of your information, should you feel it appropriate to do so. As an added precaution, we are offering you access to twelve (12) months of credit monitoring and identity theft restoration services at no cost to you. More information on these services may be found in the attached "Steps You Can Take to Protect Your Information."

**What Can You Do?** Please review the attached "Steps You Can Take to Protect Your Information." We encourage you to enroll in the credit monitoring and identity theft restoration services that we are offering as we are not able to act on your behalf to do so.

**For More Information:** We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-866-298-8060 (toll free), Monday through Friday, 6:00 a.m. to 3:30 p.m., PT.

We sincerely regret any inconvenience this incident may cause you. We remain committed to safeguarding the information in our care and we will continue to take steps to ensure the security of our systems.

Sincerely,

Handwritten signature of Jacqueline Turner in black ink, followed by the text "RN, CHP, CHC".

Jacqueline Turner, R.N.  
Covenant Care Privacy Officer

## STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

### **Enroll in Credit Monitoring**

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for twelve (12) months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit [krollbreach.idMonitoringService.com](http://krollbreach.idMonitoringService.com) to activate and take advantage of your identity monitoring services.

You have until **June 4, 2019** to activate your identity monitoring services.

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-866-298-8060. Additional information describing your services is included with this letter.

### **Monitor Your Accounts**

In addition to enrolling to receiving the complimentary services detailed above, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits, and to monitor your credit reports for suspicious activity and to detect errors. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

#### **Experian**

P.O. Box 9554

Allen TX 75013

1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 2000

Chester, PA 19016

1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

PO Box 105788

Atlanta, GA 30348-5788

1-800-685-1111

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

#### **Experian**

P.O. Box 2002

Allen, TX 75013

1-888-397-3742

[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

#### **TransUnion**

P.O. Box 2000

Chester, PA 19106

1-800-680-7289

[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

#### **Equifax**

P.O. Box 105069

Atlanta, GA 30348

1-888-766-0008

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

### **Additional Information**

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.



## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services<sup>1</sup> from Kroll:

### **Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

<sup>1</sup> Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.